UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,099	04/09/2001	Binyamin Pinkas	704-X00-47US	2969

27317 7590 10/11/2006

FLEIT KAIN GIBBONS GUTMAN BONGINI & BIANCO
21355 EAST DIXIE HIGHWAY
SUITE 115
MIAMI, FL 33180

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/807,099	PINKAS ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *23-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *27-30* is/are allowed.

6)☒ Claim(s) *23,24 and 31* is/are rejected.

7)☒ Claim(s) *25 and 26* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Chantya B. Tu
AU2135

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the RCE received on 07/20/06.

2. Claims 1-22 are canceled.

3. Claims 23-31 are newly added claims.

4. Claims 23-31 are pending.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 23-24 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ausubel (Cited in PTO 892 dated 11/02/05), in view of Micali, US Patent No. 6026163.

7. As per claims 23 and 31:

Ausubel discloses " A method for preserving the integrity of a negotiation conducted via a network, such as, the Internet, and using clients and/or servers, among a plurality of parties each of whom is making a private input during the negotiation and wherein a trusted entity acting as a center computes and outputs a value F of these inputs constituting the output of the negotiation comprising the steps of:

a) providing an architecture which includes a center A, and a plurality of participants B.sub.t, B.sub.2,..., B.sub.n, to engage in a negotiation during which all communications originating with a participant B.sub.i and transmitted to center A are exclusive" in (Fig 1, Col 24 lines 40-50, and Col 26 lines 5-20);

b) "secretly generating an input x.sub.i by each participant B.sub.i" in (Col 26 lines 20-40);

c) "publishing by the center A to each participant a commitment to K combinatorial circuits that compute F, where K is a security parameter";

d) transmitting by each participant B.sub.i to the center A a commitment c.sub.i to the value of B.sub.i's input x.sub.i, where c.sub.i is an encryption of x.sub.i;

e) "responsive to receipt of the commitments of the participants, publishing by the center A to the participants the commitments received" in (Col 26 line 65 to Col 27 line 20);

f) providing to each participant B.sub.i part of the K combinatorial circuits that the center A committed to, and requesting center A to open them, whereupon each participant B.sub.i can verify that the part of the circuits opened to participant B.sub.i computes a value F" in (Col 22 lines 30-60, and Col 27 lines 1-11);

g) transmitting by each participant B.sub.i to center A its input x.sub.i and decryption data to enable center A to verify that x.sub.i corresponds to the transmitted commitment c.sub.i" in (Col 26 lines 20-40);

h) computing by center A a value of F based on the inputs x.sub.i it received by using a part of the K combinatorial circuits not disclosed to the participants, and publishing the computed value of F to the participants" in (Col 25 line 59 to Col 26 line 4, and Col 27 lines 1-13); and

i)" transmitting to all participants a proof that the computed value of F was computed correctly, which proof can be verified by each participant using the published commitments while preventing a coalition of any one subset of participants from learning (i) anything which cannot be computed just from the output of the K combinatorial circuits and from their own inputs, and (ii) information about the inputs of other users" in (Col 27 lines 1-13).

However, Ausubel does not specifically teach of submitting the bid in a secure manner. Ausubel only refers to sealed bit in Col 21 lines 15-20.

Nevertheless, Micali discloses the "Distributed Split-Key cryptosystem and Applications" invention, which includes a method of generating a common key by calculating a combination of all participant's or bidder's public key. The common key is used by all participants or bidders to encrypt their bids and submit the encrypted bids to a center. The common key is the K security combinatorial parameter and the c.sub.i is the encrypted bids. (Col 1 line 60 to Col 2 line 16 and Col 2 lines 40-65)

Therefore, it would have been obvious at the time of the invention was made for one having skill in the art to modify Ausubel's invention to incorporate Micali's teaching of encrypting the bids with the common key to provide a secrecy of the bids until the time is right to open, to verify and to calculate the result.

8. As per claim 24:

The method of claim 23 wherein step i is carried out using a value F that is computed from the K combinatorial circuits using inputs x.sub.i and outputs j,Y of the computed value of F, F' Outputs I if and only if X(j)=Y, and X(j)>=X(i) for every i different from j" in (Col 25 line 59 to Col 26 line 4, and Col 27 lines 1-13).

Allowable Subject Matter

9. Claims 25 and 26 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. Claims 27-30 are allowed.

11. As per claim 27:

A method for preserving the integrity of a negotiation conducted via a network, such as, the Internet, and using clients and/or servers, among a plurality of parties each of whom is making a private input during the negotiation and wherein atrusted entity acting as a center computes and outputs a value F of these inputs constituting the output of the negotiation comprising the steps of:

a) announcing by center A that it will compute F;

b) providing an architecture which includes a center A, and a plurality of participants B. sub.], B.sub.2,..., B.sub.n, to engage in a negotiation during which all communications originating with a participant B.sub.i and transmitted to center A are exclusive;

c) constructing by center A K garbled circuits including gates having wire inputs and outputs that compute F;

d) choosing by center A a permutation of each wire input of the circuits;

e) publishing by center A to each participant B.sub.i tables of gates, and commitments to the permutations and the garbled values of the input wires;

f) secretly generating an input x.sub.i by each participant B.sub.i;

g) transmitting to center A, for every input wire for every circuit corresponding to an input bit known to participant B.subd, a commitment of the permuted value of the input bit;

h) responsive to receipt of the commitments of the participants, publishing by the center A to the participants the commitments received;

i) selecting by each participant B.subd a subset of the K garbled circuits that the center A committed to;

j) revealing by center A its commitments to the subset of the K garbled circuits, whereupon each participant B.sub.i can verify that the circuits revealed to participant B.sub.i computes value F;

k) verifying by participants that test circuits compute F;

1) transmitting by each participant B.sub,i to center A its input x.sub.i and decryption data to enable center A to verify that x.sub.i corresponds to the transmitted commitment in step g;

m) computing by center A a value of F based on the inputs x.sub.i it received by using circuits not in the subset disclosed to the participants, and publishing the computed value of F to the participants;

n) publishing by center A opened commitments and corresponding garbled inputs; and

o) transmitting to all participants a proof that the computed value of F was computed correctly, which proof can be verified by each participant using the published opened commitments and corresponding garbled inputs while preventing a coalition of any one subset of participants from teaming (i) anything which cannot be computed just from the output of the K garbled circuits and from their own inputs, and (ii) information about the inputs of other users.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

Thanhnga B. Do
AU2135